Information Security Policy

Section 1 - Purpose

(1) The purpose of this Policy is to ensure that the following digital information and digital information systems security objectives are achieved by the University:

a. Confidentiality – to uphold authorised restrictions on access to and disclosure of information including personal or proprietary information.
b. Integrity – to protect information against unauthorised alteration or destruction and prevent successful challenges to its authenticity.
c. Availability – to provide authorised users with timely and reliable access to information and services.
d. Compliance – to comply with relevant legislation, regulations, contractual obligations requiring information to be available, safeguarded or lawfully used.
e. Assurance – to provide assurance to the University community that information held by the University is appropriately protected and handled.

Background

(2) Data, information systems and IT Resources are strategic assets of the University and assets consequently need to be appropriately secured.

(3) This document states the University's policy on Information Security and provides requirements to establish accountability and prudent and acceptable practices regarding the use and safeguarding of the university's information resources.

(4) This Policy is closely aligned with the 2015 New South Wales Government Digital Information Security Policy as recommended for universities by the New South Wales Government ICT Strategy and draws from the following guidelines for the Information Security Industry standards:

a. AS/NZS ISO/IEC 27005:20011 Information technology — Security techniques — Information security risk management;
b. AS/NZS ISO/IEC 27002:2013(E)Information technology - Security techniques — Code of practice for information security management; and
c. AS ISO/IEC 27002:2015 Information technology — Security techniques — Code of practice for information security controls.

(5) Relevant sections from these standards are directly referenced in this Policy and accompanying Procedures.

Scope

(6) This Policy applies to:

a. the management of all matters relating to information security within the University;
b. all University information systems and information assets regardless of the media on which information is

stored, the locations where the information is stored, the technology used to process the information, or the people and roles who handle the information;

c. all Information resources owned, leased, operated, or under the custodial care of third parties operated on behalf of the University; and
d. all individuals accessing, using, holding, or managing University Information resources on behalf of the University.

Section 2 - Policy

(7) The University must have an Information Security Management System (ISMS) based on a comprehensive assessment of the risk to digital information and digital information systems.

(8) In particular, the University will:

a. manage information security with controls for access, use, storage and transmission of digital information;
b. allocate responsibility for various aspects of information security to information Owners, Custodians and Users in relation to the access, use, storage and transmission of information as described in the Information Security - Data Classification Procedure and Standards;
c. classify all information against a defined risk profile and in accordance with the Information Security - Data Classification Procedure and Standards; and
d. periodically carry out Information security risk assessments on all information systems on a regular basis in order to identify key risks and determine the controls required to effectively manage those risks.

(9) The Information Security Procedure under this Policy set rules for and explain:

a. Access Control;
b. Information Security Incident Management;
c. Information Security Requests ('Code Yellow');
d. Password Management; and
e. Information Systems Acquisition, Development and Maintenance.

(10) The Information Security - Data Classification Procedure and Standards under this Policy explain and set rules, roles and responsibilities for:

a. Data Classification Standards; and
b. Minimum Security Standards.

(11) Exceptions to the implementation of this Policy must be approved by the Chief Information Officer in consultation with the relevant University stakeholders.

Roles and Responsibilities for Information Security

(12) All Authorised Users are responsible for information security in accordance with the Acceptable Use of IT Resources Policy and this Policy.

(13) Authorised Users must:

a. use the resource only for the purpose specified by the Owner;
b. comply with controls established by the Owner; and

c. prevent the unauthorised disclosure of Confidential Data.

(14) The Chief Information Officer is the delegate authorised to take necessary action to assure continuity and security of the digital campus.

(15) Responsibility for IT Security and IT Risk rests with the Chief Information Officer and Macquarie IT Senior Leadership Team.

(16) Heads of budget divisions must:

a. actively support information security through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities;
b. ensure that all information security roles and responsibilities are clearly allocated;
c. ensure that this Policy and all supporting Procedures have been effectively implemented for their areas of responsibility; and
d. communicate to a staff member on termination their ongoing responsibilities to the University (e.g. ongoing confidentiality requirements in relation to University information assets).

(17) University budget divisions which operate IT facilities will include, amongst the duties of one or more of their staff, the role of overseeing information security and providing expert local advice as required. Specialist Information Security and IT risk management advice is available from Macquarie IT.

(18) The University will provide external providers with access to this Policy and related Procedures with which they must comply.

Compliance

(19) Macquarie IT will monitor compliance with this Policy and related Procedures. Users must promptly report breaches of this Policy and suspected information security weaknesses to the Chief Information Officer.

(20) Any breach of this Policy and related Procedures may infringe relevant legislation as listed at the outset of this Policy and expose persons to liability under such legislation.

(21) Any breach of this Policy or related Procedures may result in formal disciplinary action for students will occur in accordance with the Student Code of Conduct. Formal disciplinary action for staff will occur in accordance with the Misconduct / Serious Misconduct clauses as outlined in the Staff Code of Conduct, the Macquarie University Academic Staff Enterprise Agreement 2018 and the Macquarie University Professional Staff Enterprise Agreement 2018.

(22) Macquarie University may refer serious matters or repeated breaches to the Vice-President, People and Services, Director, Human Resources, the Head of the relevant Organisational Unit or to the appropriate external authorities which may result in civil or criminal proceedings.

(23) External providers who breach this Policy or related Procedures will be subject to suspension of access, termination of contract and / or further legal action.

Section 3 - Procedures

(24) Refer to the Information Security Procedure.

Section 4 - Guidelines

(25) Nil.

Section 5 - Definitions

(26) Commonly defined terms are located in the University Glossary. The following definitions apply for the purpose of this Policy.

(27) In this Policy, unless a contrary intention appears:

a. 'Authority' means –
    i. in relation to the IT Resources generally, the Chief Information Officer or the Chief Information Officer's delegate; and
    ii. in relation to a local facility, the relevant Head of Department, Executive Dean, or Deputy Vice-Chancellor, or a person nominated by the relevant Head of Department, Executive Dean, or Deputy Vice-Chancellor.
b. 'authorised purposes' means purposes associated with work or study in the University, provision of services to or by the University, which are approved or authorised by the relevant officer or employee of the University in accordance with University policies and procedures or pursuant to applicable contractual obligations, limited personal use, or any other purpose authorised by the relevant Authority.
c. 'Chief Information Officer' means the person holding or acting in that position in the University, or any other person nominated by the Vice-Chancellor to exercise that role for the purpose of this Policy.
d. 'Confidential Data' means one of three data classifications defined within the Data Classification Standard and Procedures. Data that is subject to restrictive regulatory obligations in relation to the access, distribution, retention and / or destruction.
e. 'Controlled Data' means one of three data classifications defined within the Data Classification Standard and Procedures. Data that is not generally created for or made available for public consumption, but that is subject to release to the public through a request via the Government Information (Public Access) Act 2009 or other applicable Commonwealth or State Law.
f. 'Data' means elemental units, regardless of form or media, that are combined to create information used to support research, teaching, and other University business processes. Data may include but are not limited to: written, electronic video, and audio records, photographs etc.
g. 'Data Center' means a facility used to house computer systems and associated components, such as telecommunications and storage systems.
h. 'Digital Data' means the subset of Data (as defined above) that is transmitted by, maintained, or made available in electronic media.
i. Director, Human Resources means the person holding or acting in that position in the University, or any other person nominated by the Vice-Chancellor to exercise that role for the purpose of this Procedure.
j. 'illegal material' means material the creation, transmission, storage, downloading or possession of which contravenes or if done in New South Wales would contravene the criminal law as it applies in any jurisdiction in Australia.
k. 'Information Security' means the protection of information and supporting systems from a wide range of threats in order to ensure business continuity, minimise operational risk, and maximise return on investments and operational opportunities.
l. 'Information Security Management System' means the policies, procedures, standards, plans, metrics, reports, resources, and services adopted for the purpose of systematically securing University Information Resources by

applying a risk management process.

m. ‘Macquarie IT’ means the Macquarie University IT Department.

n. ‘intellectual property’ includes the rights relating to –
    i. literary (including computer programs), artistic, musical and scientific works;
    ii. multimedia subject matter;
    iii. performances of performing artists, phonograms and broadcasts;
    iv. inventions in all fields of human endeavour;
    v. scientific discoveries;
    vi. industrial designs;
    vii. trademarks, service marks and commercial names and designations;
    viii. plant varieties;
    ix. circuit layouts; and
    x. confidential information.

o. ‘limited personal use’ means use that –
    i. is of a purely personal nature and not for financial gain;
    ii. does not directly or indirectly impose an unreasonable burden on any IT Resources;
    iii. does not unreasonably deny any other user access to any facilities;
    iv. does not contravene any law in any jurisdiction in Australia or any University statute, regulation, policy or procedure; and
    v. in the case of staff, does not interfere with the execution of duties.

p. 'misuse’ has the meaning set out in the Acceptable Use of IT Resources Policy Acceptable Use of IT Resources - Misuse Schedule.

q. ‘staff’ means staff of the University.

r. ‘student’ includes a person who was a student at the time of any alleged breach of this Procedure, and a person who is a student for the purposes of the Student Discipline Rules and Student Discipline Procedure.

s. ‘University copyright officer’ means the officer designated by the Vice-Chancellor as responsible for overseeing copyright issues within the University.

Status and Details

Status	Historic
Effective Date	22nd February 2021
Review Date	8th March 2021
Approval Authority	Vice-President, People and Services
Approval Date	21st June 2016
Expiry Date	28th April 2021
Responsible Executive	Eric Knight Deputy Vice-Chancellor (People and Operations)
Responsible Officer	Jonathan Covell Chief Information and Digital Officer
Enquiries Contact	Andrew Karvinen Chief Information Security Officer Information Technology